

INTERNET GUIDELINES

Over the past year, we have received many requests for clarification to the Department's Internet Policy. Specifically, folks want to know what is permissible and what is not. While the following is not intended to be a comprehensive list covering every question or concern relative to the department's Internet Policy, it does cover the more prevalent areas of concern and interest expressed. The list may change from time to time.

The Virginia Department of Social Services (VDSS) provides access to the vast information resources of the Internet to help you do your job faster and smarter. The facilities to provide that access represent a considerable commitment of department resources for telecommunications, networking, software, storage, etc. The guidelines that follow are designed to help you understand the department's expectations for the acceptable use of those resources and to help you use them wisely.

It is important for you to understand DSS's Internet usage philosophy. First and foremost, the Internet for DSS is a business tool and it is provided to you at significant cost. That means we expect you to use your Internet access for department-related purposes, (i.e., to communicate with customers and coworkers, to research relevant topics and obtain useful DSS-relevant information). You are expected to conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others. To be absolutely clear on this point, all existing department policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of resources, sexual harassment, data security, and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, and ties up printers and other shared resources. Unlawful Internet usage may also subject DSS to negative publicity and expose the department and you to significant legal liabilities.

The Internet's chat rooms, news groups and email gives each individual Internet user an immense reach to propagate department messages. Because of that power you must take special care to maintain the clarity, consistency and integrity of DSS's image and posture. Anything any one employee writes in the course of acting for the department on the Internet can be taken as representing the department's posture.

While our direct connection to the Internet offers a wealth of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. The overriding principle is that security is to be everyone's first concern. As an Internet user, you can and will be held accountable for any breaches of security or confidentiality.

GUIDELINES

Monitoring - The department has software and systems in place that can monitor and record all Internet usage. We want you to be aware that our security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No one who uses DSS's Network should have any expectation of privacy as to his or her Internet usage. Internet activity will be reviewed and usage patterns analyzed.

File Inspection - The department reserve the right to inspect any and all files stored in any areas of our network in order to assure compliance with policy.

Sexually Explicit Material - Displaying of any kind of sexually explicit image or document is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, transmitted, edited or recorded using our network or computing resources.

Web Blocking - The department uses independently-supplied screening software and data to identify inappropriate and sexually-explicit Internet sites. We block access from within our networks to all such sites. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by the screening program and notify DSS's Security Manager as to the date, time, user-ID and the name (address) of the inappropriate site.

Legal Issues - The department's Internet facilities and computing resources must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any way. Use of any department resources for illegal activity is grounds for immediate dismissal and the department will cooperate with all law enforcement bodies.

Downloading Data - (1) Any software or files downloaded via the Internet into the department's network become the property of the department. Any such files or software may be used only in ways that are consistent with their licenses or copyrights and the user must arrange to have such software properly licensed and registered. (2) You may not use the department's Internet facilities to download personal software or to download images, audio or videos unless there is an explicit business-related use for the material. (3) You may not use the department's Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.

Pirated Data - You may not use department facilities to knowingly download or distribute pirated software or data.

Malicious Activity - (1) You may not use the department's Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door program code or other

malicious program code. (2) You may not use the department's Internet facilities to knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Proper Identification - You must identify yourself honestly, accurately and completely when participating in chats or newsgroups, or when setting up accounts on any computer system.

Confidentiality - You are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential information, and any other material covered by the department's Information Security Policy. Releasing protected information will result in severe penalties as provided in the department's Information Security Policy.

Personal Use - (1) The department permits incidental use of the Internet to send and respond to personal e-mail messages; however, extensive or recurring personal use is forbidden. If you are unsure of what extensive or recurring personal use is, ask your supervisor for clarification. (2) You may not use department resources to "surf the web" for personal purposes.

Uploading Data - You may not upload any DSS- related software or data without explicit authorization from the manager responsible for the software or data.

Large File Transfers - Communications-intensive operations such as large file transfers, video downloads, mass e-mailings and the like should be scheduled for off-peak times.

Security System - DSS has installed a variety of firewalls, mail and message servers, Internet address screening programs and other security systems to assure the safety and security of the department's networks. Anyone who attempts to disable, defeat or circumvent any of these security facility or run any unauthorized network monitoring will be subject to a Standards of Conduct.

Encryption - Files that are transferred in any way across the Internet, including e-mail which contain confidential information as defined by existing data security policy, must be encrypted.

Modems - Computers that use their own modems to create independent data connections sidestep our network security mechanisms. An individual computer's private connection to any outside computer can be used by an attacker to compromise any network to which that computer is attached. For this reason any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from the department's internal networks. Major on-line services such as CompuServe and America Online can be accessed via the department's firewall-protected Internet connections making insecure direct dial-up connections generally unnecessary. Using your personal Internet Service Provider (e.g. Erols, America On Line, Hotmail, Excitemail, etc.) on a state owned PC does not release you from any of the provisions of this policy.

